TILBURG UNIVERSITY

Tilburg University

Data portability and data control

Graef, Inge; Husovec, Martin; Purtova, Nadezhda

Published in:
German Law Journal

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
Graef, I., Husovec, M., & Purtova, N. (2018). Data portability and data control: Lessons for an emerging concept in EU law. *German Law Journal*, *19*(6), 1359-1398. https://static1.squarespace.com/static/56330ad3e4b0733dcc0c8495/t/5c05ba070e2e72aaf4f621dc/1543879175464/3_Vol_19_No_06_Graef_ET_Final.pdf

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 12. May. 2021

Articles

Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*

*By Inge Graef,** Martin Husovec,*** & Nadezhda Purtova****

Abstract

The right to data portability (RtDP) introduced by Article 20 of the General Data Protection Regulation (GDPR) forms a regulatory innovation within EU law. The RtDP provides data subjects with the possibility to transfer personal data among data controllers, but has an impact beyond data protection. In particular, the RtDP facilitates the reuse of personal data that private companies hold by establishing a general-purpose control mechanism of horizontal application. Article 20 of the GDPR is agnostic about the type of use that follows from the ported data and its further diffusion. We argue that the RtDP does not fit well with the fundamental rights nature of data protection law, and should instead be seen as a new regulatory tool in EU law that aims to stimulate competition and innovation in data-driven markets.

What remains unclear is the extent to which the RtDP will be limited in its aspirations where intellectual property rights of current data holders—such as copyright, trade secrets and *sui generis* database rights—cause the regimes to clash. In such cases, a reconciliation of the interests might particularly confine the follow-on use of ported data again to specific set of socially justifiable purposes, possibly with schemes of fair remuneration. Despite these uncertainties, the RtDP is already being replicated in other fields, namely consumer protection law and the regulation of non-personal data. Competition law can also facilitate

* The research presented in this article has been conducted in the framework of a research project studying the impact of data portability on individuals, competition and innovation that received funding from Tilburg Law School and Signify. The authors would like to thank Kees Stuurman and Francisco Costa-Cabral for their valuable comments. Legislative developments up to November 9, 2018 have been taken into account.

** Assistant professor at Tilburg University, affiliated to the Tilburg Institute for Law, Technology, and Society (TILT) and the Tilburg Law and Economics Center (TILEC).

*** Assistant professor at Tilburg University, affiliated to the Tilburg Institute for Law, Technology, and Society (TILT) and the Tilburg Law and Economics Center (TILEC); affiliated scholar at Stanford University's Center for Internet and Society (CIS).

**** Associate professor at Tilburg University, affiliated to the Tilburg Institute for Law, Technology, and Society (TILT).

portability of data, but only for purpose-specific goals with the aim of addressing anticompetitive behavior.

We conclude that to the extent that other regimes will try to replicate the RtDP, they should closely consider the nature of the resulting control and its breadth and impact on incentives to innovate. In any case, the creation of data portability regimes should not become an end in itself. With an increasing number of instruments, orchestrating the consistency of legal regimes within the Digital Single Market and their mutual interplay should become an equally important concern.

A. Introduction

As a part of its Digital Single Market Strategy, the European Commission committed to developing a European data economy.[1] Data has been acknowledged as an essential resource for economic growth, and it is estimated that by 2020 the size of the EU data economy may increase to €739 billion—or 4% of the overall EU GDP.[2] Against this background, the regulation of the allocation of and extent of control over data—by way of exclusive rights or possibilities of access—becomes increasingly important. Put differently, the shape and direction of data flows—as well as varieties of data-enabled business models and the ways of drawing value from data—will depend on multiple factors. These include: who gets access to data and under what circumstances; who is precluded from access; who can move or keep their data assets to itself; and who is obliged to share data with others. Data portability, namely "the ability to move, copy or transfer" data,[3] is one of the instruments of such control.

A significant share of the data circulating in the digital economy is the data relating to identified or identifiable natural persons, which constitutes "personal data" in the sense of EU data protection law. Against this background, the new GDPR[4] introduces a regulatory innovation: RtDP in relation to personal data. Under Article 20 of the GDPR, an individual to whom the data relates—a data subject[5]—has a right to receive a copy of personal data pertaining to him or her—in a structured, commonly used, and machine-readable format—

---

[1] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a Digital Single Market Strategy for Europe* 14, COM (2015) 192 final (May 6, 2015).

[2] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building a European Data Economy*, COM (2017) 9 final (Jan. 10, 2017).

[3] *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy, Accompanying the Document Communication Building a European Data Economy* 46, SWD (2017) 2 final (Jan. 10, 2017).

[4] Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) (EU) [hereinafter GDPR].

[5] *See id.* art. 4(1) (defining a data subject as "an identified or identifiable natural person" and specifying that

> an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . . .)

In this article, the terms "data subject," "individual," "consumer," and "user" will be used interchangeably.

and to transmit this data to, in the data protection parlance, another "controller"—namely any person or legal entity who determines the purposes and means of data processing.[6]

To illustrate, users of the online music streaming service *A*, in theory, should be able to demand exportation of their personal data such as music preferences, and import it into music streaming service *B*. The RtDP will inevitably affect the landscape of control over personal data, both in relations between the users of digital services and the service providers and in relations between competitors on the market of digital services. Since the GDPR and the new RtDP have become effective on May 25, 2018,[7] this article provides a much-needed mapping and study of anticipated issues in the implementation of the new right.

The objective of this article is two-fold. On the one hand, the article aims to examine the allocation, nature, and extent of control over personal data that will result from the RtDP as introduced in the GDPR. On the other hand, the article extrapolates these findings beyond Article 20 of the GDPR and pays attention to the rise of data portability as an emerging concept in regimes of EU law other than data protection. As such, rather than providing concrete answers as to the desired scope of data portability, the article gives an overview of the current state of data portability in EU law and raises issues that need to be considered in the future development of the concept.

The article proceeds in the following steps. Part B gives a short overview of the legislative history of the RtDP under Article 20 of the GDPR. Part C examines from a data protection perspective the nature and extent of individual control conferred by Article 20 of the GDPR, which introduces the RtDP and sets out its scope and limitations. Part D then continues the this analysis by exploring the RtDP's interface with intellectual property ("IP") and possible market outcomes. IP might in some situations re-define the aspirations of the RtDP as a general-purpose regime. In addition, the competitive impact of the RtDP is vital to understand its side consequences on markets beyond the individual as the primary beneficiary under the GDPR. Part E approaches data portability from a broader perspective by exploring the extent to which data portability can be facilitated on the basis of other regimes next to Article 20 of the GDPR, namely competition and consumer protection law. Based on this analysis, Part F concludes by offering lessons which should inform any future general-purpose regimes for data portability like the GDPR.

The article puts forward that the RtDP of the GDPR is a first attempt to establish a general-purpose control mechanism of horizontal application that will mainly facilitate the sharing and reuse of data. While a sector-specific form of portability applies in some

[6] *Id.* art. 4(7).

[7] *Id.* art. 99.

industries—for instance, in telecom and banking[8]—the GDPR introduces for the first time a horizontal regime that will apply across sectors to the economy as a whole. Unlike current initiatives in consumer protection law, RtDP does not confer ownership-like control over ported data, but rather facilitates control for the purposes of reuse. We submit that it also does not unequivocally belong within the scope of the fundamental right to data protection but should rather be regarded as a tool to stimulate competition and innovation. Despite the regulatory silence, IP law will be relevant both by creating limitations on the RtDP of data subjects under the GDPR and by safeguarding control claims of businesses regarding their interests over datasets against competitors. When IP rights of current data holders—such as their copyright, trade secrets, and *sui generis* database rights—cause the two regimes to clash, a reconciliation of the different interests might limit the free follow-on use of ported data under the RtDP again to a purpose-specific context. This generalist approach with ex-post correction through balancing contrasts with competition law, which may also impose limitations as to how firms use and control data to compete. Unlike the GDPR—which provides data subjects with an RtDP of a general scope which can be invoked against any data controller irrespective of the purpose for which portability is sought—competition law can be used only to facilitate data portability on a case-by-case basis for specific goals remedying identified and proved competition concerns. When we look beyond these two regimes, we can observe an increasing number of initiatives that seem to be replicating the GDPR's generalist design. Based on the analysis of Article 20 of the GDPR, we offer lessons for data portability as an emerging regulatory innovation spreading to different fields of EU law.

B. Legislative History of the Right to Data Portability

To adequately interpret the RtDP under EU data protection law, it is worthwhile to consider its evolution in legislative history from origin to final adoption. The RtDP in data protection law was introduced by the European Commission in January 2012 in the proposal for a GDPR.[9] The new right was one of the instruments by which the Commission

[8] *See* Directive 2002/22/EC of the European Parliament and of the Council of March 7, 2002 on Universal Service and the Rights of Users Relating to Electronic Communications Networks and Services (Universal Service Directive), 2002 O.J. (L 108) 51, as amended by Directive 2009/136/EC of the European Parliament and of the Council of November 25, 2009, 2009 O.J. (L 337) 11 (stating that under Art. 30 of the Universal Service Directive, porting of telephone numbers and their subsequent activation has to take place against a cost-oriented price and within the shortest possible time which is interpreted as maximum one working day); *see also* Directive 2015/2366 of the European Parliament and of the Council of November 25, 2015 on Payment Services in the Internal Market, 2015 O.J.(L 337) 35 (EU) (stating that under Art. 66 and 67 of the Payment Services Directive 2 to be implemented in national law by January 13, 2018, third party providers are able to access a customer's payment account information on the customer's request in order to provide payment initiation or account information services).

[9] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, COM (2012) 11 final (Jan. 25, 2012).

sought to restore trust in online services. By enabling data subjects to transfer personal data among data controllers, the Commission aimed to ensure individual control over personal data held by service providers.[10]

The subsequent review of the Commission's proposal in the European Parliament led to the adoption of numerous amendments contained in the legislative resolution of March 2014.[11] As a result of some of these amendments, the RtDP was merged with the right of access. Even though the principles underlying the original RtDP that the Commission proposed remained unchanged in the amended proposal, the European Parliament expressed the view that the RtDP should be seen as a mere extension of the right of access rather than a right of its own. Ultimately, in the final version of the GDPR as adopted by the European Parliament and the Council in April 2016, the RtDP was again included in a separate article.[12]

Before its final adoption, the RtDP had to overcome a critical review by the Council, where several member states expressed doubts as to whether it should be retained in the GDPR. A number of member states pointed to the risks of data portability for the competitive positions of companies and raised issues about the relationship between commercial confidentiality and the IP of data controllers. Some member states even considered data portability not to be within the scope of data protection, but rather in consumer or competition law.[13] Nonetheless, as the new right aimed to increase the control of data subjects over their personal data and to ensure the free flow of personal data between member states, it was eventually considered to fall within the ambit of an EU data protection instrument. In the end, the RtDP survived the negotiations in the Council and was included as Article 20 of the GDPR. A clause in Article 20(4), stating that the RtDP "shall not adversely affect the rights and freedoms of others," was included to remedy possible harmful effects on the interests of third parties.

---

[10] *Commission Staff Working Paper Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) and the Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data*, at 43, SEC (2012) 72 final [hereinafter *Impact Assessment*].

[11] Resolution on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), EUR. PARL. DOC. P7_TA(2014)0212 (2014) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212.

[12] *See* GDPR, *supra* note 4, art. 20.

[13] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COD (2014) 10614/14 (June 6, 2014) 3 n.1.

As the final wording of the RtDP leaves open quite a number of issues regarding its scope and implementation, the Article 29 Working Party (WP29)[14] published draft guidelines in December 2016, discussing the new right and clarifying the conditions under which it is applicable.[15] After a public consultation—in which stakeholders were given the opportunity to comment on these draft guidelines—WP29 issued its final guidelines on April 5, 2017.[16] The guidance aimed to prepare controllers who have had to start applying the RtDP and the GDPR as a whole as from May 25, 2018.[17]

While the main policy objective of the Commission behind the introduction of the RtDP was to ensure that individuals are in control of their personal data and trust the digital environment, it is clear that the new right may also reduce lock-in by enabling users to switch easily between services. As a result, the RtDP could foster competition between controllers as a side-effect and thereby encourage the development of new data-related services. As such, the new right interacts with other legal fields such as competition and IP law. As already hinted above, interactions with IP law may put restrictions on the extent to which data subjects may effectively invoke their RtDP. Considering the hybrid nature of the RtDP, one can raise the questions of how it fits with the fundamental right to data protection and what the nature of control is that it aims to ensure.

C. The Right to Data Portability and Individual Control

The RtDP is indeed strongly connected to the rhetoric of individual control that dominated the data protection reform efforts. According to Recital 68 of the final version of the GDPR, the RtDP shall "further strengthen [data subjects'] control" over their personal data. In its April 2017 guidelines specifying the scope of the new right and the conditions of its application, WP29 similarly notes that "[t]he primary aim of data portability is *enhancing individual's control* over their personal data and making sure they play an active role in the data ecosystem."[18] This Section will explore how data portability delivers on this promise.

---

[14] WP29 is composed of the following parties: a representative from the National Data Protection Authority of each EU Member State; a representative of the European Data Protection Supervisor (the independent supervisory authority that is responsible for ensuring that all EU institutions and bodies respect people's right to personal data protection and privacy when processing their personal data); and a representative of the European Commission.

[15] Art. 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, 16/EN WP 242 (Dec. 13, 2016).

[16] Art. 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, 16/EN WP 242 rev.01 (Apr. 5, 2017) [hereinafter WP29].

[17] *See, e.g.*, GDPR, *supra* note 4, art. 99(2).

[18] WP29, *supra* note 16, at 4 n.1 (emphasis added).

I. Nature of Control: Fundamental Rights, Data Ownership, and Sharing

What is the nature of control that data portability ensures? The forthcoming analysis will examine this from three–not mutually excluding–angles: (1) how data portability relates to the fundamental right to data protection and the related rhetoric of control; (2) control as data ownership; and (3) control to enable data sharing. It is argued that the kind of control data portability grants does not unequivocally belong within the scope of the fundamental right to data protection. At the same time, data portability does not create ownership-like control over personal data; its nature can instead be best defined by reference to the data sharing and reuse that it facilitates.

1. Data Portability and the Fundamental Right to Data Protection

Data portability is often connected to control over personal data as part of the fundamental right to data protection under Article 8 of the EU Charter of Fundamental Rights [hereinafter the Charter]. This connection is based on the legislative history of the GDPR. According to the Commission, one of the three general objectives of the reform was "[t]o increase the effectiveness of the fundamental right to data protection," which implied, among others, "that individuals are in control of their personal data and trust the digital environment."[19] The Commission considered data portability as instrumental to ensuring such control and the effectiveness of the fundamental right of Article 8 of the Charter.[20] Therefore, data portability appears to be regarded by the Commission as part of the fundamental right to data protection. This interpretation is further supported by the non-binding explanation of the EU Network of Independent Experts on Fundamental Rights.[21]

Yet, Article 8 of the Charter does not explicitly mention data portability or control, while it does explicitly contain parallels with other provisions of the GDPR. The general clause of Article 8(1) envisages simply that "[e]veryone has the right to the protection of personal data." The qualifying provisions in Article 8(2) further specify that "[s]uch data must be processed fairly for specified purposes"[22] and on the basis of the consent or another legitimate ground laid down by law;[23] that everyone has the right of access to data[24] and

[19] *Impact Assessment*, *supra* note 10, at 62.

[20] *Impact Assessment*, *supra* note 10.

[21] *See EU Network of Independent Experts on Fundamental Rights Commentary of the Charter of Fundamental Rights of the European Union*, at 95 (June 2006), http://ec.europa.eu/justice/fundamental-rights/document/index_en.htm (stating, namely, that secondary legislation is adopted to give effect to the fundamental right to data protection, and that "the protection of personal data shall be exercised in accordance with the conditions and limits defined by the measures adopted to give effect to it.").

[22] *See* GDPR, *supra* note 4, art. 5(1) (a), (b) (featuring a parallel structure).

[23] *See id.* at art. 6, 9.

the right to rectification.[25] Finally, Article 8(3) states that "[c]ompliance with these rules shall be subject to control by an independent authority."[26]

Neither can the RtDP be regarded as an extension of the right of access explicitly mentioned as protected under Article 8(2) of the Charter.[27] The scope of the RtDP goes beyond access in some aspects—for instance in what is provided to the data subject and in what format—and in others falls short—for instance in the limited range of situations in which it is applicable. While the right of access grants only a right to receive a confirmation of data processing and a copy of data undergoing processing "in a commonly used electronic form,"[28] data portability enables the data subject to receive a copy for own use and to transmit the data to another controller in a "structured, commonly used and machine-readable" format,[29] making data portability especially suitable for the digital context. At the same time, compared to the right of access which is of general application, the broader data portability right is applicable only in a reduced number of situations. It can be invoked only regarding the data "provided" by the data subject to the controller,[30] and only when processing is automated[31] and based on consent[32] or on a contract.[33]

These observations raise doubt about whether data portability falls within the scope of Article 8 of the Charter, as well as about the fundamental rights nature of the kind of control the new RtDP is giving.[34] The relationship between data portability and Article 8 of the Charter fits within a larger discussion of the relationship between the Data Protection Directive and the GDPR, on the one hand, and Article 8 of the Charter, on the other hand.

---

[24] *See id.*at art. 15.

[25] *See id.* at art. 19.

[26] *See generally id.* at art. 51.

[27] *See* Charter of Fundamental Rights of the European Union, 2012/C 326/02, art. 8(2), 2012 O.J. (C 326) 391 ("Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.").

[28] *See* GDPR, *supra* note 4, art 15(1), (3).

[29] *See id.* at art 20(1).

[30] *See* discussion *infra* Section C.II. on the notion of provided data.

[31] *See* GDPR, *supra* note 4, art. 20(1)(b).

[32] *See id.* at art. 6(1)(a), 9(2)(a).

[33] *See id.* at art. 6(1)(b).

[34] *But see* Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, 42(6) EUR. L. REV. 793, 809–10 (2017) (claiming that the right to data portability "sits coherently within the data protection regime" because it promotes individual control over personal data by enhancing informational self-determination as "a central objective of the EU data protection regime.").

2. Data Portability and Data Ownership

A number of scholars suggest that data portability is closely akin to the property-rights approach to data protection or data ownership.[35] These authors, however, seem to focus on what Rubinstein calls "property-related actions like trading, exchanging, or selling data,"[36] rather than the defining element of property rights—namely the right to exclude. This meaning of the concept "property" is not attached to any one jurisdiction, but derives from studies in comparative European property law. Property thus is any interest in an object, tangible or intangible, that is directed against the entire world (has a so-called *erga omnes* effect).[37] Alienability, or the ability to trade, is therefore not a necessary defining characteristic of property.[38] The RtDP as a property right would enable the data subject to take his or her data and leave a digital platform or service. Article 20 of the GDPR, however, alone or in combination with the right to erasure, does not create such a right to exclude.

Data portability and erasure are two independent rights under the GDPR; when the RtDP is invoked, it does not automatically trigger a request for erasure.[39] While the two requests can be aligned and filed at the same time—for instance in case the data subject withdraws its consent for the processing—the alignment is not perfect. This is due to the limited scope of application of the right to erasure and a wide range of situations following from Article 17(1) and (3) GDPR, where the request for erasure may be left unsatisfied. For instance, a data subject cannot obtain erasure of personal data by withdrawing consent when the controller can justify processing on another ground under Article 6 GDPR—namely contract or legitimate interest of the controller.

[35] *See, e.g.*, Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L., 74–87 (2013); *see also* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 373 (2013); Paul De Hert et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 COMPUT. L. & SEC. REV. 193, 201 (2018).

[36] Rubinstein, *supra* note 35, at 84.

[37] NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE 57 (2011).

[38] *Id.* at 86–88; *but see* Elinor Ostrom & Charlotte Hess, *Private and Common Property Rights*, *in* 5 PROP. L. & ECON. 53, 59 (Boudewijn Bouckaert ed., 2010) ("Property-rights systems that do not contain the right of alienation are considered to be ill-defined.").

[39] WP29, *supra* note 16, at 7.

3. Portability for Data Sharing and Reuse

What seems to characterize the function of data portability more accurately is granting control of the kind that enables free flow of data among controllers, namely data sharing and reuse. Similarly, Drexl argues that the right to data portability should be considered as a tool of access enabling individuals to switch where access to data is crucial for competition.[40] The RtDP consists of two elements: (1) the right to obtain a copy of data, and (2) the right to transmit data to another controller, also directly. In the latter regard, Article 20(2) GDPR states that "the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible." Recalling the Guidelines on data portability of WP29, "[t]he primary aim of data portability is enhancing individual's control . . . and making sure they *play an active role in the data ecosystem*."[41] As WP29 interprets it, in addition to preventing service lock-ins, the RtDP "[i]n essence . . . is expected to foster opportunities for innovation and sharing of personal data between data controller . . . under the data subject's control."[42]

The emphasis on data sharing and reuse is reinforced by the requirement for the format of transmitted data. In accordance with Article 20(1) GDPR, it has to be "structured, commonly used and machine-readable," aiming to produce interoperable systems.[43] WP29 suggests the use of Application Programming Interfaces ("APIs") to facilitate automated data portability.[44] The automated RtDP will enable business models either assisting individuals with their data management or capitalizing on reuse of personal data collected by others. WP29 explains that the use of APIs "would enable individuals to make requests for their personal data via their own or third-party software or grant permission for others to so do on their behalf (including another data controller) . . . ."[45]

Preventing lock-ins and promoting innovation by reuse may be broadly supported purposes of regulation, and the ability of data subjects to share and reuse their data may constitute a form of control over data. Such power is meant to be general-purpose control in the sense that the law does not confine the exercise of the control with some types of socially beneficial activity or social goals. In this sense, it is completely "purpose agnostic." Yet one can doubt: first, if this kind of control that aims at more intensive data (re)use

---

[40] Josef Drexl, *Designing Competitive Markets for Industrial Data — Between Propertisation and Access*, 8 JIPITEC 257, 286, para. 155 (2017).

[41] WP29, *supra* note 16, at 4 n.1 (emphasis added).

[42] *Id.* at 5.

[43] *Id.* at 4, 14.

[44] *Id.* at 15.

[45] *See generally* WP29, *supra* note 16.

belongs with data protection and its roots in privacy; and second, like Koops asks, if data protection law is the right place to address all data-related problems.[46]

II. Extent of Control: Processing Grounds and Data Types

Having established that the nature of control data portability grants is limited to data sharing and reuse, this Section will demonstrate that the extent of such control is also limited: (1) in terms of the conditions of processing that allow data portability, and (2) in terms of the kinds of data that can be ported.

1. Scope Limitations Concerning Processing Grounds

It has already been noted that the impact of the RtDP will likely be limited because the right can be invoked only—following Article 20(1) GDPR—with regard to personal data processed based on consent[47] or on a contract[48].[49] This caveat effectively excludes an obligation for the controller to provide a copy of the data processed under all other grounds, including legitimate interest.[50] This raises the question whether controllers will be able to preclude data subjects from relying on the RtDP by invoking a legitimate interest as a ground for processing personal data instead of consent or a contract.

Article 20(3) and Recital 68 GDPR explicitly exclude portability of data when processing is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." The reason behind the latter caveat is unclear because data processed by public authorities has already been made available for reuse via open data initiatives harmonized by the PSI Directive.[51] The PSI Directive created a clear obligation for member states to make all documents reusable in a machine-readable format, albeit without prejudice to data protection law and subject to

[46] Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIVACY L., 250–61 (2014).

[47] *See* GDPR, *supra* note 4, art. 6(1)(a), 9(2)(a) (specifying this point for special categories of data).

[48] *See id.*

[49] Colette Cuijpers et al., *Data Protection Reform and the Internet: The Draft Data Protection Regulation*, *in* RESEARCH HANDBOOK ON EU INTERNET LAW 543, 558 (Andrej Savin & Jan Tzarkowski eds., 2014).

[50] *See* GDPR, *supra* note 4, art. 6(1)(f).

[51] Directive 2003/98/EC of the European Parliament and of the Council of November 17, 2003 on the Re-Use of Public Sector information 2003 O.J. (L 345) 90, last amended by Directive 2013/37/EU of the European Parliament and of the Council of June 26, 2013 2013 O.J. (L 175) 1 [hereinafter PSI Directive] (stating that the amendments are in effect from July 18, 2015).

exceptions.[52] Both Article 20 of the GDPR and the arrangements of the PSI Directive are without prejudice to national regimes and their access to documents.[53] Therefore, the purpose of preventing abuse of rights—namely the use of data portability to create a back-door right of access to the documents of public authorities where such a right does not exist—does not work as a justification for the exclusion of personal data held by public authorities from the scope of the RtDP.

Nevertheless, WP29 suggests making data portability arrangements as a matter of good practice when data portability is not mandatory under Article 20 of the GDPR, for instance when data is processed by public authorities or for legitimate interest.[54] The recommendation concerning the processing for legitimate interest might be of a more persuasive authority, given that the availability of data portability tools needs to be taken into account when assessing if legitimate interest under Article 6(1)(f) of the GDPR is a suitable processing ground—for instance, when balancing interests of the controller with rights and interests of others.[55]

2. Scope Limitations Concerning Data Types

As the scope of the GDPR is limited to the processing of personal data, only personal data—namely information relating to a natural person who is identified or identifiable by means reasonably likely to be used—can be subject to a data portability request. Truly anonymous data is excluded. Given the progress in data analytics, the range of data that falls under the definition of personal data expands[56]—and so in principle should the range of situations where data portability can be invoked. At the same time—in line with Article 11(1) of the GDPR—data controllers are not required to maintain data in an identifiable form solely to meet portability requests. When data is pseudonymous—namely the data can be attributed to a specific data subject only with additional information[57]—data controllers are not required to re-identify, unless the data subject "provides additional

[52] PSI Directive, *supra* note 51, at art. 4; *but see id.* at recital 8, 9 of the preamble (explaining that article 4 does not apply if access is, for instance, restricted or excluded under national access rules and due to third-party interests).

[53] *See* CJEU, Joined Cases C-141/12 and C- 372/12, YS et al. v. Minister of Immigration, Integration and Asylum, ECLI:EU:C:2014:2081, Judgement of July 17, 2014 (concerning the relationship between data protection rights and the right to access to documents).

[54] WP29, *supra* note 16, at 8 n.16.

[55] *Id.* (referring to the relevant pages of WP29, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC," April 9, 2014, WP217).

[56] *See, e.g.*, Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, 10 LAW, INNOVATION & TECH. 40–81 (2018) (discussing the broad notion of personal data).

[57] *See* GDPR, *supra* note 4, art. 4(5).

information enabling his or her identification," as specified in Article 11(2) GDPR. Read together, Articles 20 and 11 GDPR may motivate controllers to opt for processing pseudonymised datasets to avoid the obligations of data portability when they are unwilling to share—for instance to preserve their unique datasets. At the same time, frequent use of Article 11(2) may lead to more frequent identification of data subjects. Though meant to facilitate data reuse, it would potentially reduce anonymity and pseudonymity in other contexts.

While controllers may freely choose to facilitate portability of all data, the more impactful and debated scope limitation is that the enforceable right exists only for data the data subject "provided to the controller" under Article 20(1)'s first indent. The GDPR does not provide an explanation as to the meaning of "provided." Hence, this provision can be construed in various ways.[58]

(1) In the narrowest sense, "provided data" would mean data volunteered, or actively disclosed by the data subject—for instance by filling in a form or answering a questionnaire.

(2) A broader interpretation would also include data that is "passively provided," or observed, by use of equipment or service provided by the controller.

(3) The broadest interpretation would include all data processed by the controller on the grounds of contract or consent. Such interpretation can be based on the idea that data processing on the grounds of contract to which the data subject has agreed and consent of the data subject imply that the data is provided by the data subject.

WP29 chose a middle ground and interprets "provided data" as the "data actively and knowingly provided by the data subject" and "observed data provided by the data subject by virtue of the use of the service or the device."[59] The observed data includes a person's search history, traffic and location data, other raw data—such as the heartbeat tracked by a wearable device—,[60] and generally "all data observed about the data subject during the activities for the purpose of which the data are collected."[61] Examples of the latter are "transaction history or access log, . . . [d]ata collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track

[58] *See also* De Hert et al., *supra* note 35, at 202 (distinguishing between a restrictive and an extensive approach to data portability).

[59] WP29, *supra* note 16, at 10.

[60] *Id.*

[61] *Id.* at 10 n.21.

browsing behavior)."[62] While WP29 explains that "provided" should be interpreted broadly, the term should exclude data that is "inferred" and "derived"—and thus created by the controller, such as via an analysis of provided data[63]—like assessments, profiles, scores, etc.

While WP 29 most likely makes this distinction to balance data portability with the IP rights of controllers, its origins have nothing to do with IP. This classification of data seems to be adopted from the World Economic Forum and OECD discussions concerning privacy, and was first made during the OECD privacy expert roundtable in 2014.[64] The experts then distinguished data that is provided, observed, derived, and inferred; the difference between the last two was that derived data was created in a "mechanical" way "to detect patterns . . . and create classifications" in a manner "not based on probabilistic reasoning," while inferred data was "product of probability-based analytic processes."[65] The World Economic Forum adopted the classification merging the last two categories into one, "inferred", to raise awareness as to the scale of personal data processing, and the various types of personal data that area processed.[66]

The blurry conceptual boundaries of provided data will undoubtedly cause difficulties for the data subjects when invoking the RtDP. For instance, it is not clear what degree of controller input on top of the raw data will take data out of the scope of portability. While some cases are clearer—individual credit scores and profiles, for instance—others are not. Think of a photograph uploaded onto a photo sharing platform using a platform-provided filter. At the same time, an incidental benefit of this limitation is that controllers who are unwilling to share will be motivated to delete raw data when its processing is no longer strictly necessary.

---

[62] *Id.*

[63] *Id.* at 10.

[64] Org. for Econ. Co-operation and Dev. [OECD], *Summary of the OECD Privacy Expert Roundtable on Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking* 5 (Mar. 21, 2014), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en; *see also* World Econ. Forum, *Rethinking Personal Data: A New Lens for Strengthening Trust* 5 (May 2014) http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

[65] OECD, *supra* note 64, at 5.

[66] *Id.*

III. Silent Conflict with IP Rights

The RtDP is subject to further limitations in the interests of third parties as laid down in Article 20(4) GDPR. These could be data protection rights of other platform users[67] but also IP rights—particularly copyright protecting software and trade secrets.[68] The GDPR is silent on the extent of the conflict with these interests. While the RtDP creates incentives to reuse data, it might limit incentives to create or collect them.

One may argue that limiting the RtDP to "provided data," as opposed to data that is "derived" or "inferred", is a result of regulatory balancing of a data protection right and the IP rights conducted by the legislator. This would for instance prevent competitors from benefiting from ready consumer profiles or reverse-engineering of an algorithm from inferred data. Yet, WP29 provided further guidelines on how to balance the RtDP with IP rights when complying with GDPR. For instance, when discussing the data format, WP29 suggests that the data should be provided "along with useful metadata at the best possible level of granularity" and that "[t]his metadata should be enough to make the function and reuse of the data possible but, of course, without revealing trade secrets."[69] At the same time, "the result of those considerations should not be a refusal to provide all information to the data subject" and "data controllers can transmit the personal data . . . in a form that does not release information covered by trade secrets or IP rights."[70]

Interestingly, in the absence of an IP-specific clarification in Recital 68, WP29 seems to base its interpretation on Recital 63, which provides an explanation to the limitation of the right of access under Article 15(4):

A data subject should have the right of access . . . and to exercise that right easily and at reasonable intervals . . . That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.[71]

---

[67] *See* WP29, *supra* note 16 (devoting substantial attention to how data protection rights of other data subjects should be respected when portable data concerns data subjects other than the one invoking the RtDP—think of the contact lists or email recipients).

[68] *Id.* at 12.

[69] *Id.* at 18.

[70] *Id.* at 12.

[71] *See* GDPR, *supra* note 4, at recital 63 of the preamble (emphasis added).

That WP29 draws an analogy between the right of access and the RtDP when it comes to the interface with IP rights is understandable, given the RtDP's legislative history and its historical link to access. In addition, the outcome of this analogy is favorable to the RtDP: "the result of those considerations should not be a refusal to provide all information to the data subject."[72] WP29 appears to assume that requested data can be easily stripped of its IP components:

> [a] potential business risk cannot . . . in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transfer the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.[73]

Yet, we contend that WP29 underestimates the extent of potential conflict between the RtDP and the IP rights. The interplay with existing IP rights is and will be more complex in practice. IP and data portability rights will touch and they will have to be reconciled. In the next Section, we examine these conflicts more closely.

D. The Right to Data Portability, IP Law and Consequences

The previous Section showed that Article 20 of the GDPR aspires to achieve general-purpose reallocation of control over privately held data, subject to some conditions. Rather than a tool to further the objectives of data protection law, the RtDP seems to aim mainly at stimulating competition and innovation in data-driven markets. As such, its application raises questions about how the RtDP will interact with the incentives of firms to innovate and compete. While the RtDP's regulatory DNA lies in improving access to privately held personal data, access to data through portability has a flip side for the addressees—the private parties collecting, analyzing, and trading in the data. Beyond mere compliance, the instrument acts as a push measure by forcing the private party to disclose, at least, a certain type of data and to share it with others upon the request of the data subject. This possibility undoubtedly influences the business strategy and potentially also market incentives concerning data creation and reuse which will be discussed in this section.

I. Place in Innovation Policy

The state can play several roles in supporting data-enabled innovation. Apart from creating a general ecosystem of economic and political institutions, the state may: (1) offer IP rights

[72] WP29, *supra* note 16, at 12.

[73] *Id.*

in data as an incentive for data creation and reuse; (2) intervene on the side of demand[74]—for instance through prizes, or supply[75]—as was done in the PSI Directive; or (3) improve its institutions to better facilitate some form of market exchanges. Data portability instruments constitute an active intervention on the side of supply of information under point (2). Such intervention, however, interferes with other policies, in particular rewards promised through IP rights under point (1).

IP rights are usually the most systemic intervention, as they reflect the government's belief that incentives can induce further production or commercialization for the entire class of innovation. For that reason, IP rights usually come equipped with an exclusivity prerogative that makes certain types of uses of a protected investment subject to the consent of right holders. Right holders are then expected to commercialize them through markets, either on their own or through licensing. Three basic IP rights will likely be relevant for the relationship between IP law and the RtDP under the GDPR.

Copyright is an exclusive right that protects original expressions, mostly coming from the domain of art and science.[76] Such expressions can include photos, blog entries, tweets, sounds, or reviews. *Sui generis* database right protects databases which are a result of substantial investment in the collection, verification, or presentation of its data.[77] This can include datasets that were tediously collected or cleaned, such as collections of user reviews and preferences. The exact investment threshold differs among the member states, but investments as low as 4,000 EUR were accepted to suffice in some countries.[78] Last but not least, trade secrets protect commercial information which has an economic

[74] In the area of data-enabled innovation, the state could offer prizes or research grants to facilitate or speed-up certain types of innovations.

[75] Public Sector Information (PSI) is an area where the state actively promotes reuse of data which is produced by the governments and its agencies. PSI policies—see the PSI Directive—are meant to spur broader availability of such data. This is supporting supply of information for data applications—such as travel navigators.

[76] *See* Directive 2001/29/EC, of the European Parliament and of the Council of May 22, 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10 [hereinafter InfoSoc Directive]; *see also* CJEU, Case C‑5/08, Infopaq Int'l A/S v. Danske Dagblades Forening, ECLI:EU:C:2009:465, Judgement of July 16, 2009.

[77] *See* Directive 96/9/EC, of the European Parliament and of the Council of March 11, 1996 on the Legal Protection of Databases 1996 O.J. (L 77) 20 [hereinafter Database Directive]; *see also* CJEU, Case C-203/02, British Horseracing Board Ltd. V. William Hill Organization Ltd., ECLI:EU:C:2004:695, Judgement of November 9, 2004.

[78] *See* BGH, Dec. 1, 2010, I ZR 196/08, https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=ddaeb8a77db54f5f3e77f66c04e774ff&nr=56329&pos=0&anz=1 (explaining that the German Federal Court of Justice accepted the amount of 4,000 EUR as sufficient); *see also*, Martin Husovec, *The End of (Meta) Search Engines in Europe?*, 14 CHI.-KENT J. OF INTELL. PROP. 145, 145–72 (2014) (discussing the different thresholds across the EU).

value to a firm owing to its secrecy.[79] Protected subject matter can include lists of customers, their shopping habits, and preferences or pricing strategy. Each right comes with a different set of exclusive rights. Copyright protects—among other things—against unauthorized reproduction and communication to the public.[80] *Sui generis* database right protects against extraction and reutilization of substantial part of the database, or also of its insubstantial part if made systematically.[81] And trade secrets protect against unlawful acquisition of secrets obtained through unauthorized access, appropriation, or any other conduct which, under the circumstances, is considered contrary to honest commercial practices.[82]

To be sure, many data assets held by firms will not qualify for any IP protection because they do not meet the required threshold of protection.[83] Such data assets are IP-free.[84] Requesting such information does not conflict with any IP right. A firm facing such disclosure will not be able to object to it on the basis of exclusive IP rights.[85] IP-

[79] Directive 2016/943, of the European Parliament and of the Council of June 8, 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use, and Disclosure, 2016 O.J. (L 157) 1 [hereinafter Trade Secret Directive].

[80] *See* InfoSoc Directive, *supra* note 76, art. 2, 3.

[81] *See* Database Directive, *supra* note 77, art. 7.

[82] *See* Trade Secret Directive, *supra* note 79, art. 4(2).

[83] *See generally* Herbert Zech, INFORMATION ALS SCHUTZGEGENSTAND (2012); *see also* Herbert Zech, *Information as Property*, 6 JIPITEC, 192 (2015).

[84] At the moment, there is an ongoing policy debate and a lot of academic interest in ownership of data discussing who owns data, when and whether we need to introduce new exclusive rights, such as a right of data producers. *See* European Commission, *Legal Study on Ownership and Access to Data,* SMART No. 2016/0085 (2016); *see also* Anette Gärtner & Kate Brimsted, *Let's Talk About Data Ownership*, 39 EUR. INTELL. PROP. REV., 461, 461–66; *see also* Daria Kim, *No One's Ownership as the Status Quo and a Possible Way Forward: A Note on the Public Consultation on Building a European Data Economy*, 13 J. OF INTELL. PROP. L. & PRAC., 154 (2017).

[85] It might still invoke, however, a right to conduct business. *See* GDPR, *supra* note 4, art. 20(4). Such objections are probably less likely to be persuasive than ones backed with existing IP rights. This is because any ownership of this information is not a result of legal allocation by means of exclusive rights, but only a mere consequence of the service's set-up, such as its technological design coupled with market power leveraged through contract law. The grey area between IP-encumbered and IP-free data might be information which are not covered by any exclusive rights but can be protected against misappropriation through unfair competition laws. Unless such tortious claims qualify for protection as a form "intellectual property" under Art. 17(2) of the Charter, they might be taken into account only within a right to conduct a business. Today, such doctrines are not harmonized on the EU level, and differ greatly across the countries. *See* Ansgar Ohly, *Interfaces Between Trade Mark Protection and Unfair Competition Law: Confusion About Confusion and Misconceptions About Misappropriation?*, *in* INTELLECTUAL PROPERTY, UNFAIR COMPETITION AND PUBLICITY: CONVERGENCES AND DEVELOPMENT 33 (Nari Lee et al. eds., 2014); *see also* Dirk Visser, *Misrepresentation and Misappropriation: Two Common Principles or Common 'Basic Moral Feelings' of Intellectual Property and Unfair Competition Law*, *in* COMMON PRINCIPLES OF EUROPEAN INTELLECTUAL PROPERTY LAW 247, 247–54 (Ansgar Ohly ed., 2012).

encumbered assets, however, will benefit from the fundamental rights protection offered by Article 17(2) of the Charter. But, with what consequences? WP29 argues that "[t]he right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights."[86]

Of the three rights, copyright might be the easiest to strip from any data assets for the purposes of compliance. In practice, we can encounter four basic scenarios: (1) copyright is held by the data subjects; (2) copyright is held by the platform which either owns it originally (own creations) or on the basis of transfer/exclusive license; (3) copyright ownership is mixed for the content at stake; or (4) the copyright is held by third parties, such as friends who made pictures. As most of the platforms do not ask for transfer of rights or exclusive licenses for user-generated content, a lot of provided content will be owner by users. For sui generis database rights, such a distinction will be much more difficult. This is because sui generis rights are created as an additional layer of protection independently of materials such as texts, sound, images, numbers and facts—which are systematically or methodically arranged. The data controller, as a database maker, owns his exclusive rights regardless of the parallel rights the data controller holds. Structures as simple as XML or PDF were classified as a database in the case law.[87] In the case of trade secrets, the same applies. The fact that information is provided by the user, does not exclude it from forming a basis of broader trade secret right.

As such, IP rights send a signal to their beneficiaries that the activity they engage in will be rewarded through exclusive rights. The rights as such should ease recouping the costs of the investment. Data portability policies can conflict with this signal in several ways when data is IP-encumbered. The following three areas might be the main areas of daily friction. First, mandatory portability can force disclosure of data that could otherwise be kept away from competitors and thus preserved as an advantage in the process of competition. Second, it can prescribe sharing of data where exclusivity was previously promised as a reward. Third, it can undermine revenue that the potential beneficiary expected from her licensing activity and thus broadly innovation incentives. In the following Sections, we will analyze how the data portability regime embodied in Article 20 of the GDPR specifically interfaces with IP policies in this regard. It is argued that this general-purpose regime can easily become, at least in some situations, much more purpose-limited due to IP rights protecting the exclusivity of data.

GDPR's RtDP comes with four important innovations. First, the data must be provided in "structured, commonly used and machine-readable format." This allows scalability. Second, data subjects have a right to "transmit those data to another controller without

[86] WP29, *supra* note 16, at 12.

[87] *See* Technomed Ltd. v. Bluecrest Health Screening Ltd. [2017] EWHC (Ch) 2142 [75].

hindrance."[88] This allows aggregation and reuse. Third, the original data controller—addressee of the request—is obliged to provide such information free of charge. This allows experimentation and lowers barriers to entry. Fourth, the regime aspires to achieve general-purpose access to privately held data. This means no extra evidence or justification is needed to mandate access. These four aspects might prove crucial in triggering the use of the instrument. Taken together with the scope of Article 20 of the GDPR, they will also have a defining impact on how the right will interact with IP rights. The fourth aspect might, however, become less pronounced in situations where a conflict between IP rights and the instrument will be encountered.

II. Exclusivity of Data Assets

IP rights lend exclusivity to their beneficiaries. Copyright and *sui generis* database right define acts which third parties cannot undertake without the permission of beneficiaries. Data portability guarantees that the data controller—and an unlimited number of third parties of his/her choice—might reuse the information for whatever purpose. Hence if the data asset is copyright protected—e.g., text of an email or a picture—, the situation can arise where, on the one hand, copyright law guarantees exclusivity of use to a piece of data and data portability, on the other hand, foresees possibility of its reuse. How will such conflict be resolved? Is the GDPR's RtDP merely *lex posterior* or *lex specialis* that always overrides IP rights, or is Article 20(4) meant to invite to open-ended case-by-case reconciliation of the two?

Two different situations must be distinguished in this regard: (1) disclosure and use by the data subject; and (2) use by the subsequent new data controllers. Moreover, what will matter in both cases, as this generally matters for IP law, what is the purpose of use of the data asset.

If we agree with the WP29's position on analogical application of Recital 63 to Article 20 of the GDPR, we could conclude that only adverse effects can compromise goals of data portability. This suggests somewhat higher standard than mere "interference."[89] Moreover, then, the full refusal of information should be an extremely uncommon outcome of the balancing exercise—if possible at all. This suggests that counter-weighing justification would have to be very intensive to curtail the scope of initial disclosure and use by the data subject under point (1). No comparably strong language is found with regard to its reuse by subsequent data controllers under point (2). The condition "without hindrance" seems to apply to technical transfer of data. It is not entirely clear if it could also encapsulate conditions of its reuse. If this is not the case, then it would mean that

[88] *See* GDPR, *supra* note 4, art. 20(1).

[89] *See* Martin Husovec, *Trademark Use Doctrine in the European Union and Japan*, 21 MARQ. INTELL. PROP. L. REV. 1 (2017) (explaining that in trademark law, "adverse effect" has its use in the area of trademark functions).

while point (1) is very hard to limit on the basis of IP rights, point (2) might be more common. It cannot, however, be ruled out that without hindrance assumes a broader meaning that generally steers the conflicts in favor of data protection.

Could IP nevertheless impose limits on disclosure and use by the data subject himself/herself? The data subject's social interest is stronger than one for its reuse by others. Private analyses of one's own data can be more closely linked to data subject's expression of personality and his/her sense of privacy than its subsequent commercial reuse. Moreover, more exceptions and limitations might cover such unauthorized uses. For some IP rights—such as copyright laws—exceptions for private use might exempt such uses anyway, so the conflict might be less pronounced. Therefore, IP rights are generally less likely to prevail in this area.[90]

The situation might be more complex with regard to new subsequent data controllers. Their use is an expected consequence of a general-purpose data portability right but is also further away from the control rationale.[91] This prompts the question about the obligations of follow-on data controllers regarding the original controller's IP rights. To illustrate the tensions, consider the following examples. A user of a review website uploads her selfies from a vacation along with her review to the website, giving a non-exclusive license to the service without a possibility to sub-license. She is the copyright owner of the selfie or text and the service became its non-exclusive license. When she decides to export her data and import them with another service, relying on Article 20 of the GDPR, there is no conflict because the website's rights are not in play. This would change, however, if the user and the service arrange for an exclusive license under which the service is the only entitled entity to exploit the copyrights in the text—thus becoming an exclusive copyright licensee. This can happen in the context of services that invest in user's content by giving them something in exchange—for instance, discounts or remuneration.[92] In such a situation, the user and others can be theoretically excluded from use of the text based on copyright law

---

[90] *See* Till Jaeger, *Legal Opinion – Legal Aspects of European Electricity Data*, JBB RECHTSANWÄLTE (2017), https://open-power-system-data.org/legal-opinion.pdf (discussing the limits on follow-on use of energy data).

[91] *See* WP29, *supra* note 16, at 4 ("The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another.").

[92] At the moment, an exclusive licensee seems like a rare model. Many services take a non-exclusive license with a possibility to sub-license. *See* Steven Hetcher, *User-Generated Content and the Future of Copyright: Part Two - Agreements Between Users and Mega-Sites*, 24 SANTA CLARA HIGH TECH. L. J. 829, 847 (2008) (discussing Facebook's Terms of Service); *Terms of Service*, FACEBOOK (Apr. 19, 2018), https://www.facebook.com/terms.php; *see also TripAdvisor Widget Terms of Use*, TRIPADVISOR (Sept. 2017), https://www.tripadvisor.com/pages/widget_terms.html; *Terms of Service*, AIRBNB (Apr. 16, 2018), https://www.airbnb.com/*terms*; *Twitter Terms of Service*, TWITTER (May 25, 2018), https://twitter.com/en/tos; *Terms of Service*, YOUTUBE (May 25, 2018), https://www.youtube.com/static?template=terms&gl=US. Sometimes, however, the borderline between the user's and site's content can be murky.

(save for statutory exceptions), but remain free with regard to the picture. The RtDP allows the user to obtain the text and encourages to use it in a private sphere. Moreover, it allows the user to transmit it to any other service. Nevertheless, if such a service starts using the picture in the sense of copyright law,[93] the question is whether it must acquire a license from the original data controller who holds the right.

A similar situation might arise with respect to the sui generis database right. The original data controller could have invested heavily in attracting certain type of user-information—for instance, consumer reviews of purchased products. As long as some of those reviews qualify as personal data—and are aggregated from several users—competing services would be able to extract and reutilize protected parts of the database. Again, such reuse by competitors directly intrudes into the exclusive right of a database maker—the original data controller. Just consider the example of Albert Heijn presented below. Will follow-on controllers have to seek a license to such a database, or will they be exempted? Moreover, what happens when the original IP rights owners, be it the copyright licensee in the first example or the database maker in the second, refuse to grant consent?

It is clear that allowing exclusivity to take precedence over the reuse of ported information might endanger the policy goals of Article 20 of the GDPR. What benefit does a "right to transmit without hindrance" offer if it can be torpedoed by IP rights? In the area of IP, exceptions and limitations are always strictly tied to the purpose of the use of a given asset. This is probably most obvious when looking at the copyright landscape, which constrains any exceptions to a pre-defined catalogue of social causes.[94] The mutual conflict of the RtDP and IP will not escape this reality. Therefore, the resolution will inevitably be use-specific as well. As a consequence, a general-purpose regime like the GDPR can break into a purpose-specific regime for reuse as soon as it hits IP rocks on its way. This would limit incentives for reuse.

III. Disclosure of Data Assets

Data portability by definition promotes disclosure of data. Such disclosure can, however, conflict with a firm's plans to keep information secret in order to leapfrog competitors or prevent them from imitating its independently developed innovation. To give an example, shopping habits and history of customers constitute both personal data and trade secrets.[95] They are collected for the purposes of safeguarding customer loyalty and

[93] For simplicity, assume a safe harbor scenario, such as the application of art. 14 of the E-Commerce Directive.

[94] *See* InfoSoc Directive, *supra* note 76, art. 5.

[95] As an illustration, Facebook has already invoked trade secret protection as a justification for not disclosing all personal data in response to an access request of an individual user. The social network provider claimed that one of the sections of the Irish Data Protection Acts, to which Facebook is subject because its international headquarters are in Ireland, "carves out an exception to subject access requests where the disclosures in

improving the quality of services or products. Although portability does not necessarily lead to public availability of data, Article 20 of the GDPR can in practice lead to sufficient relevant availability to data subjects and third parties that were entrusted with the reuse. Such parties certainly can include direct or indirect competitors. As a consequence, convincing the data subjects to request their data through general-purpose regimes could become a way for competitors to challenge each other's data assets. It is easy to imagine how, for instance, energy suppliers start persuading their competitor's customers to invoke portability regarding their past consumption in exchange for discounts if they switch to their own offering. Moreover, a user's access to some of his or her consumption patterns as a type of observable data can lead to increased technological and business opportunities for personalized comparative advertising—e.g., consumption-pattern based comparison of prices.

For instance, imagine a supermarket chain, such as Albert Heijn, that invests lot of money in convincing its customers to use its loyalty card. It offers customers special deals, promotes its use in advertising, and trains its employees to actively ask for the card while customers are paying. Such a card typically collects the full consumption pattern of a consumer, which is of great value and might qualify for protection under the *sui generis* database regime, or as a trade secret. A competing chain, such as Lidl, might be interested in luring the customers and offer them an easy option to simply compare the prices if they start shopping at its stores. Lidl uses ported data—falling within the scope of Article 20 of the GDPR—and summarizes the prices that would be paid for comparable products in its store. The result is greater market transparency, but also deterioration of Albert Heijn's investment in collecting the data.

Firms in the EU are entitled to trade secret protection as long as such information has a commercial value because of its secrecy and its owner takes reasonable steps to keep it secret.[96] Unlike patent law, trade secret protection does not lend exclusive rights against the use of trade secrets that result from an independent discovery or market observation.[97] This means that right holders cannot prohibit the use of their secrets if other firms arrive at them by investing in their own research and development. This includes a possibility to deduce them from an observation or testing of lawfully acquired products of their competitors.[98]

---

response would adversely affect trade secrets or intellectual property." *See* Email from Facebook to Max Schrems, (Sept. 28 2011), http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf.

[96] *See* Trade Secret Directive, *supra* note 79, art. 2(1).

[97] In IP scholarship, there is lively debate about whether trade secrets are a form of "intellectual property." *See* Lionel Bentley, *Trade Secrets: "Intellectual Property" but not "Property?"*, *in* CONCEPTS OF PROPERTY IN INTELLECTUAL PROPERTY LAW 60 (Helena Howe & Jonathan Griffiths eds., 2013) (arguing that they are predominantly being accepted as "intellectual property," but not "property").

[98] *See* Trade Secret Directive, *supra* note 79, art. 3.

How far-reaching Article 20 of the GDPR is in limiting the expectation of a firm's sphere of secrecy depends on the construction of its scope.[99] The effect on data secrecy seems to be twofold—direct and indirect—depending on how the instrument influences it. While direct effects take away secrecy by curbing it, the indirect effect broadens factual and legal possibilities of its lawful disclosure.

First, the direct effect concerns all the data that are considered "the personal data concerning [the data subject], which he or she has provided to a controller." Only this type of data can be subject to a successful request for disclosure. The information obtained can then be transmitted to third parties or reused by the data subject. Such disclosure or subsequent use is secrecy-destroying when it can be said that otherwise protected information now became "generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question."[100]

The disclosure towards the data subject could be interpreted either: (1) as automatically secrecy-destroying; or (2) potentially secrecy-destroying.

If we were to accept the first reading, it would mean that data portability would in fact never directly conflict with the right to trade secrets. It conflicts only with the expectation of secrecy. By limiting the remit of possible secrecy, it curtails the effective scope of where trade secret rights might arise or be maintained. A parallel can be drawn with consumer transparency regimes, under which companies are asked to publicly disclose some information. Under such reading, portability or transparency obligations strip firms of possibilities to preserve secrecy about certain aspects of their business. As such, Article 20 of the GDPR would co-define what can qualify as a trade secret—and thus IP—within the meaning of Article 17(2) of the Charter.

If we were to accept the second reading, Article 20 of the GDPR would be secrecy-destroying only where the entitled data subject requested protected information and simultaneously entrusted its reuse with a third party which comes from "within the circles that normally deal with the kind of information in question."[101] This would mean that trade secrecy rights arise over subjected assets, and continue to exist despite compliance with the request based on Article 20 of the GDPR until the point when relevant circles effectively acquire such information. Only at such moment would trade secret rights evaporate. If the analysis proceeds in this way, then the argument can be made that imminent disclosure based on Article 20 of the GDPR has a potential to endanger further

[99] *See supra* Section C.II.

[100] *See* Trade Secret Directive, *supra* note 79, art. 2(1)(a).

[101] *See id.*

existence of trade secret rights and must be balanced against the right itself—provided that they qualify under protection of Article 17(2) of the Charter.[102] Such analysis would have to be made on a case-by-case basis. The adoption of any of two viewpoints might affect where the line of balance with secrecy is drawn.

In any case, data portability also may have an indirect impact on trade secrecy. This impact is perhaps even more significant. Because the RtDP targets provided information, which is interpreted as input and observed data about the data subject, this data is less likely to be the most economically indispensable for the firm. Such accessibility of input and/or observed data, however, can help to reverse-engineer otherwise unreachable data—for instance inferred data—which is not subject to portability. By being able to analyze the exact input/observed data of the service together with the resulting services might provide for better chances of uncovering the key trade secrets. The data portability might thus help to broaden the factual scope of reverse engineering which in consequence again limits trade secret rights.

IV. Licensing Revenue from Data Assets

Exclusivity rarely constitutes an end in and of itself for firms. More often, firms engage in licensing through which they exchange their prerogative against monetary compensation. Therefore, even in situations where the right holder will be forced to relinquish any right to authorize follow-on use of their protected data assets, firms might still benefit from such compensation. The fact that right holders are obliged to respect the reuse of information by other firms does not imply that such reuse of data must remain without remuneration. Article of the 20 GDPR does not mention any fees. Unlike the right of data access,[103] it does not link the exercise of the right to any obligation to reimburse the original data controller under some circumstances. As a result, the general clause of Article 11(5) of the GDPR applies which states that actions taken to comply with data subjects' rights shall be provided free of charge, unless requests from a data subject are manifestly unfounded or excessive (in particular because of their repetitive character). In the latter cases, the controller may charge a reasonable fee taking into account administrative costs. Free-of-charge provision of data, however, does not automatically mean that the *reuse* of IP rights must also be without any monetary compensation.

Arguably, one of the ways to achieve balancing would be to reconcile goals of IP rights with goals of data portability by means of establishing an occasional condition of fair remuneration. This would effectively mean that the RtDP is allowed to operate and be

[102] *See also* Bentley, *supra* note 97, at 77 (discussing the Veolia case and whether disclosure would be in conflict with Article 8 ECHR or Article 1 of the First Protocol of the ECHR).

[103] *See* GDPR, *supra* note 4, art. 15(3) ("For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.").

used. But if it is relied on by third parties who would otherwise have to seek a license to use the assets, they would not be exempted from an obligation to pay fair remuneration. Such schemes that promote access to technology and IP rights exist in the area of standardization.[104] Here, they are the result of private commitments by firms that participate in the standardization process and hold patent rights that read on implementation of the standards. A balancing exercise between Article 20 of the GDPR and IP rights could take these private ordering schemes as an inspiration to reconcile two policies in cases where IP rights are closely tight to the revenue of firms.[105]

This is not to say that such remuneration schemes should always be the result of such balancing. It is to say only that its possibility, as a middle ground, will prevent less polarized thinking about the conflicts between the two interests. It also means that recognized remuneration interests will not be sufficient to prevent disclosure and reuse. In this sense, such schemes can broaden the effects of data portability policies when applied to IP-encumbered data assets. From the perspective of many IP rights, the goals are still achieved when an obligation to pay substitutes exclusivity. In the area of IP, many private ordering or legislative solutions exist that sometimes transform a right to exclude into a less intrusive right to be paid.[106] This can potentially reduce incentives to create, collect, and clean the data. The need for any incentives to induce such activities otherwise than by market competition, however, is largely disputed.[107]

Nonetheless, the concept of fair remuneration is not without administration costs. It would almost certainly lead to several complications. First, there is a lot of hope that the RtDP can be standardized. In order to achieve scalability and automation, this must happen. The more case-by-case considerations there are, the more difficult it is to embody them into standardized solutions. It is already hard to identify IP-encumbered assets, as some of the protection thresholds—such as substantive investment—are invisible to an outside observer.[108] Perhaps the solution would be similar to the area of patent licensing of standard-essential patents[109]—to simply put the burden of the first step onto the right

---

[104] *See generally JRC Science and Policy Report on Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms*, (2015), http://is.jrc.ec.europa.eu/pages/ISG/EURIPIDIS/documents/05.FRANDreport.pdf.

[105] Inge Graef & Martin Husovec, *Response to the Public Consultation on "Building a European Data Economy,"* TILBURG LAW SCHOOL RESEARCH PAPER SERIES No. 10/2017 (Apr. 25, 2017) (discussing this trade-off between short term and long term).

[106] Examples include private levies for private reproduction, licensing through collective management organizations, FRAND-licensing in the area of standardization, compulsory licensing, etc.

[107] *See* Drexl, *supra* note 40; *see also* P. Bernt Hugenholtz, *Something Completely Different: Europe's Sui Generis Database Right*, *in* THE INTERNET AND THE EMERGING IMPORTANCE OF NEW FORMS OF INTELLECTUAL PROPERTY (Susy Frankel & Daniel Gervais eds., 2016); Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, GRUR INT. 989, 989–98 (2016); Husovec, *supra* note 78, at 145–72.

[108] *See* Husovec, *supra* note 78, at 145–72 (discussing this aspect in the context of database *sui generis* right).

[109] CJEU, Case C-170/13, Huawei Technologies Co. v. ZTE Corp., ECLI:EU:C:2015:477, Judgement of July 16, 2015.

holders who in licensing disputes must first alert the alleged infringer of the infringement complained about and clarify which patent and how it was infringed. Nonetheless, one should think about the practicality of technical and institutional set-up of the market surrounding such a licensing exchange before embarking on this path of balancing.

V. Impact on Data-Driven Markets

It is clear that Article 20 of the GDPR will have an impact beyond individual data subjects who can invoke the RtDP. By imposing restrictions on the extent to which market players can process personal data, data protection law structures markets and influences the competitive process. As such, most data protection rules raise entry barriers to the data economy because they subject the collection and use of personal data to additional requirements. The RtDP, however, can also make it easier for market players to collect personal data and thereby facilitate market entry. In its Guidelines on Data Portability, WP29 explicitly stated that the RtDP "is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers."[110] As such, markets could become more open to new entrants and thus more competitive by making the control incumbents have over data less durable.[111] While the RtDP stimulates competition and thereby can have a positive impact by facilitating diffusion and reuse of data, it also imposes a compliance burden on market players.[112] Article 20 of the GDPR will apply to all controllers irrespective of their size, the scale of their processing activities, and the purpose for which portability is sought. The RtDP may pose some problems, as every sector will face its own difficulties with regard to its implementation. In some sectors, key players already provide their users with certain functionalities for exporting data—in the form of services like Facebook's Download Your Info and Google Takeout.[113] In other

[110] WP29, *supra* note 16, at 3.

[111] *See also* Lynskey, *supra* note 34, at 804–06.

[112] *See* Swire & Lagos, *supra* note 35, at 352; *see also Legal Memo with Respect to the Article 29 Guidelines on the Right to Data Portability*, EUROPEAN TELECOMMUNICATIONS NETWORK OPERATORS' ASSOCIATION 8–9, (Feb. 16, 2017) https://etno.eu/datas/positions-papers/2017/170131%20ETNO_Data%20Portability_Memo/170131%20ETNO_Data%20Portability_Memo.pdf [hereinafter ETNO Memo] (arguing that the interpretation of the RtDP as put forward by WP29—namely that the concept of data "provided by the data subject" includes not only data actively and knowingly inserted by a data subject, but also data obtained by observing the behavior of a data subject—places a disproportionate obligation on telecom operators which are already subject to portability duties under the EU framework for electronic communications).

[113] *See Accessing & Downloading Your Information*, FACEBOOK (2018) https://www.facebook.com/help/131112897028467; *see also Download Your Data*, GOOGLE, https://takeout.google.com/settings/takeout; *see also Introducing Data Transfer Project: an open source platform promoting universal data portability*, GOOGLE OPEN SOURCE BLOG (Jul. 20, 2018), https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html (stating that in July 2018, Google Facebook, Microsoft and Twitter announced the Data Transfer Project which is "an open source initiative

sectors, like telecommunications,[114] any such relevant experience is lacking and no interoperable standards and formats are yet available. Does the RtDP create an obligation for market players to develop and agree upon a common format if none exists yet? This remains open.

As a general-purpose regime, Article 20 of the GDPR may have a broader impact on the competitive landscape. In particular, it remains to be seen whether access to ported data under the RtDP will create a level playing field or whether instead incumbents will continue to retain a competitive advantage. This could be due to the continuous access to the real-time flow of first-hand data that incumbents possess, as opposed to ad hoc second-hand data access of new entrants. It should also be noted in this regard that the data access of new entrants is dependent on whether individual data subjects invoke their RtDP. The new right gives only individuals the right to receive and transfer data to a new controller. As such, the RtDP is not concerned with the ability of businesses themselves to directly get access to data in order to compete on a market.[115] In this sense, data subjects remain in control, although, as was explained earlier, they can be easily seduced and instrumentalized by businesses.

Moreover, because the RtDP will apply horizontally, new entrants and incumbents alike are able to use it for their respective ends. As a result, the impact on competition may go both ways. On the one hand, data portability may foster competition, facilitate reuse of ported data, and stimulate the creation of innovative data analytics services.[116] In this regard, it is important to keep in mind that the RtDP will not only enable the transfer of data to a direct competitor, but also facilitates users to take advantage of complementary, value-added services such as product comparison services.[117] On the other hand, some measure of standardization and interoperability of data formats—as well as data processing procedures—might be required in order to make portability meaningful. Standardization can help to implement the RtDP in a cost-effective way and thus increase its positive effects. A possible negative consequence of standardization, however, is that once a particular standard is chosen, the development of new technologies stagnates. This is because market players will be inclined to provide products and services complying with

---

dedicated to developing tools that will enable consumers to transfer their data directly from one service to another, without needing to download and re-upload it.").

[114] See ETNO Memo, *supra* note 112, at 7–8.

[115] *See* Aysem Diker Vanberg & Mehmet Bilal Ünver, *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?*, 8 EUR. J. OF L. & TECH. 1, 2 (2017).

[116] *See also* Rubinstein, *supra* note 35, at 80.

[117] *See* Barbara Engels, *Data Portability Among Online Platforms*, 5 INTERNET POL'Y REV. 6–10 (2016) (making a distinction between platforms offering substitute and complementary services when examining the possible impact of the right to data portability on competition and innovation).

the agreed standard.[118] While the exact impact of the RtDP on the competitive landscape remains to be seen, it is clear that its implementation will influence innovation incentives and innovation paths depending on the breadth of its scope of application as well as the resolution of its trade-off with IP rights.

E. Data Portability as an Emerging Concept Beyond the GDPR

From the perspective of EU law, it is important to note that the RtDP is not an isolated phenomenon. An increasing number of initiatives are emerging to replicate the GDPR's generalist design in the area of consumer protection law and free movement law. In this Section, we first explore the only pre-GDPR regime that facilitated portability—competition law—and in turn look at designs of other upcoming policies and their internal and external consistencies.

I. Data Portability and Competition Law

The possible enforcement of data portability under competition law differs from the way in which the RtDP is to be implemented under data protection law. First, it is important to note that the GDPR gives data subjects a right to data portability, while competition authorities can impose a duty on dominant providers to enable data portability in case their behavior amounts to abuse under Article 102 of the TFEU. Second, the scope of application of the two regimes is different. As it forms part of a data protection instrument, the RtDP naturally applies only to transfers of personal data. Information that does not qualify as personal data prima facie falls outside the scope of the new right. In addition, a data subject is entitled to only port personal data which he or she has provided to a controller under Article 20(1) GDPR. Regardless of how this phrase will eventually be interpreted,[119] it is clear that such a limitation does not play a role in the enforcement of competition law.

Under competition law, action can potentially be taken against a lack of portability of any data, irrespective of whether it relates to an identified or identifiable natural person and whether it is provided by this person as long as it qualifies as anticompetitive behavior. The scope of application of competition law in this regard is thus much wider. At the same time, it must be kept in mind that action on the basis of Article 102 of the TFEU—the most relevant provision for enforcing data portability under competition law—can be taken only if the restrictions on data portability qualify as abuse of dominance with the specific

[118] *See* Francisco Costa-Cabral & Orla Lynskey, *Family Ties: The Intersection Between Data Protection and Competition in EU Law*, 54 COMMON MKT L. REV. 11, 39 (2017) (arguing that standard-setting to ensure a good functioning of the right to data portability "may necessitate an agreement between competitors and therefore entail a potential violation of Article 101 TFEU").

[119] *See* discussion *supra* Section C.II. regarding the concepts of derived and inferred data.

purpose of remedying harm to competition.[120] In contrast, the RtDP will apply generally to all forms of processing carried out by automated means and based on consent or on a contract irrespective of the purpose for which portability is sought.[121] No dominance or abuse will need to be established for users to be able to transfer their data under the GDPR.[122]

Both data protection and competition law can thus be used to facilitate data portability, albeit in different ways. While data protection law grants individual data subjects a RtDP vis-à-vis data controllers in general, a competition intervention is only possible when a lack of data portability leads to competitive harm in the specific circumstances of the case. Unlike data protection law—which protects individual data subjects—competition law is concerned with protecting consumer welfare more broadly by safeguarding the competitive process to benefit consumers, competitors, and the economy as a whole. By intervening against anticompetitive practices, competition enforcement aims to keep markets open and protect consumers by ensuring a genuine choice of good quality products and services. The application of competition law is, however, triggered only in the presence of actual, proven competition problems. This explains why the resulting remedy adopted under competition law will be purpose-specific.

Even before the GDPR was adopted, former Competition Commissioner Almunia made clear in a speech that the RtDP "goes to the heart of competition policy," and that "portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them."[123] By stating "[w]hether this is a matter for regulation or competition policy, only time will tell," he acknowledged the right to data portability as a new tool under data protection law but at the same time did not eliminate competition law intervention for facilitating data portability.[124] The European Commission or national competition authorities therefore may also intervene on the basis of competition law if a dominant firm does not allow users to take their data with them when switching services.[125]

---

[120] *See also* Lynskey, *supra* note 34, at 801–02 (comparing the personal and material scope of the GDPR right versus the competition law remedy of data portability).

[121] These are the preconditions for the right to data portability to apply under Art. 20(1)(a) and (b) GDPR.

[122] *See* MARC BOURREAU ET AL., BIG DATA AND COMPETITION POLICY: MARKET POWER, PERSONALISED PRICING AND ADVERTISING 25 (2017), http://cerre.eu/sites/cerre/files/170216_CERRE_CompData_FinalReport.pdf (comparing enforcements of data portability on the basis of data protection and competition law in).

[123] Press Release, Joaquin Almunia, Competition Comm'r, European Comm'n, Remarks on Competition and Personal Data Protection at the Privacy Platform Event: Competition and Privacy in Markets of Data in Brussels, (Nov. 26, 2012), http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.

[124] *Id*.

[125] *See, e.g.*, Inge Graef et al., *Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union*, 39 TELECOMM. POL'Y 502, 508–09 (2015); *see also* Inge Graef et al.,

The *Facebook/WhatsApp* merger decision—in which the Commission assessed whether data portability issues constituted a barrier to the switching of consumers in the context of consumer communications applications—is instructive in this perspective. The Commission made clear that it had not found any evidence suggesting that this was indeed the case. According to the Commission, communication via apps tends to consist to a significant extent of short and spontaneous chats which do not necessarily carry long-term value for consumers. The Commission also considered that the messaging history remains accessible on a user's smartphone even if the user starts using a different communications app. Finally, the Commission took into account that the contact list can be easily ported because a competing application—after obtaining consent of the user—would get access to his or her phone book on the basis of which existing contacts can be identified.[126] Even though the Commission did not consider restrictions on data portability to constitute barriers to switching in the specific circumstances of the case, the fact that these issues were investigated under merger review illustrates the potential of competition law to address data portability.

This can be further illustrated by the *Google* abuse of dominance case in which the Commission previously negotiated with Google about commitments which would force the search engine provider to stop imposing obligations on advertisers preventing them from moving their advertising campaigns to competing platforms.[127] In the United States, the Federal Trade Commission closed its investigation when Google offered voluntary concessions to remove restrictions on AdWords that made it difficult for advertisers to manage advertising campaigns across multiple platforms.[128] By restricting the possibility of advertisers to move their campaigns to another advertising platform, providers create switching costs that may cause advertisers to stay with their current provider solely because they find it too cumbersome to manually re-insert their advertising campaign in a new platform. This case shows that competition authorities on both sides of the Atlantic are ready to remedy a lack of data portability as a competition issue.

Putting the Right to Data Portability into a Competition Law Perspective, LAW. J. OF THE HIGHER SCH. OF ECON. ANN. REV. 7–8 (2013).

[126] Case No COMP/M.7217, October 3, 2014, paras. 113–15, 134, 2014 O.J., http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

[127] For Commitments of Google, see Case COMP/C-3/39.740 *Foundem and others,* April 3, 2013, paras. 27–31, 2013 O.J., http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_8608_5.pdf; *see also* Joaquin Almunia, Competition Comm'r, European Comm'n, *Remarks on the Google Antitrust Case: What is at Stake?*, (Oct. 1, 2013), http://europa.eu/rapid/press-release_SPEECH-13-768_en.htm (stating that Google offered improved commitments to the Commission which included a new proposal providing stronger guarantees against circumvention of the earlier commitments regarding portability of advertising campaigns).

[128] *Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns in the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search*, FTC (Jan. 3 2013), http://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc.

In particular, a refusal of a dominant firm to facilitate data portability may constitute a form of abuse by exploiting consumers or excluding competitors. A lack of data portability may exploit consumers when it restricts their choice of competing offers. In the context of exclusionary abuse, a lack of data portability may lead to barriers of entry for competitors and violate Article 102(b) of the TFEU by limiting markets and technical development to the prejudice of consumers.[129] Data portability may also be adopted as a remedy to address related exploitative or exclusionary abuses and thus be used as a tool to restore competition in the market. For instance, a requirement of data portability could remedy an exploitative abuse consisting of the excessive extraction of personal data from consumers.[130] By forcing a dominant provider to give users the possibility to transfer their data to a competitor, a competition authority can thus address relevant exploitative or exclusionary abuses. Beyond portability, a duty to share data can be imposed on a dominant firm under Article 102 of the TFEU if the strict requirements of the so-called essential facilities doctrine are met.[131] In particular, the data has to be indispensable for competitors to introduce their own products or services on the market.[132] In a merger setting, remedies of data portability or data sharing may play a role as tools to prevent a merger from "significantly imped[ing] effective competition."[133] The remedy adopted by the Commission in the 2008 *Thomson/Reuters* merger decision provides precedent for such an approach. The Commission approved the merger on the condition that the merging parties would divest copies of their databases containing financial information. This remedy would allow purchasers of the databases to quickly establish themselves as a credible competitive force in the marketplace in competition with the merged entity.[134]

---

[129] *See* Christopher Yoo, *When Antitrust Met Facebook*, 19 GEO. MASON L. REV. 1147, 1154–55 (2012); *see also* Damien Geradin & Monika Kuschewsky, *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue* 11, (SSRN Working Paper, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088.

[130] *See* Francisco Costa-Cabral, *The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law*, 23 MAASTRICHT J. EUR. AND COMP. L. 495, 511 (2016).

[131] *See* INGE GRAEF, EU COMPETITION LAW, DATA PROTECTION AND ONLINE PLATFORMS: DATA AS ESSENTIAL FACILITY 249–80 (2016) (discussing in detail the application of the essential facilities doctrine to data).

[132] *See, e.g.*, CJEU, Joined Cases C-241/91 and C-242/91, Radio Telefis Eireann and Indep. Television Publ'ns Ltd v. Comm'n of the European Communities, ECLI:EU:C:1995:98, Judgement of April 6, 1995; CJEU, Case C-7/97, Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs, ECLI:EU:C:1998:569, Judgement of November 26, 1998; CJEU, Case C-418/01, IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, ECLI:EU:C:2004:257, Judgement of April 29, 2004; CJEU, Microsoft Corp. v. Comm'n of the European Communities, Case T-201/04, ECLI:EU:T:2007:289, Judgement of September 17, 2007.

[133] Council Regulation (EC) 139/2004 of Jan. 20, 2004 on the Control of Concentrations Between Undertakings (EU Merger Regulation), art. 2(3), 2004 O.J. (L 24) 1, 7.

[134] Case No COMP/M.4726 February 19, 2008, 2008 O.J., http://ec.europa.eu/competition/mergers/cases/decisions/m4726_20080219_20600_en.pdf.

The extent of control over data that competition law may give thus amounts to the imposition of certain limitations on market players as to how they use their datasets to compete.[135] Competition law can play an important role in promoting data portability and data sharing as well, although its scope is limited to a case-by-case analysis of competition concerns. Because of their potential to facilitate data access and reuse more widely, general-purpose data portability regimes, such as Article 20 of the GDPR, may restructure markets beyond what competition law is able to achieve with its case-by-case approach. At the same time, competition authorities do have a certain margin of discretion to adopt remedies that relate to the identified competition concerns once the competition rules are triggered. This is particularly the case in two scenarios. In a merger setting, the merging parties are dependent on the discretion of the competition authority to prevent the merger from being blocked. As a result, the authority has scope to require remedies that have a broader impact on the market, as long as they can be linked to the identified competition concerns.[136] Where undertakings offer commitments to end a competition investigation without establishing an infringement, there is even more room for competition authorities to do so. The Court of Justice has made explicit in *Alrosa* that undertakings proposing commitments "consciously accept that the concessions they make may go beyond what the Commission could itself impose on them" in an infringement decision.[137] If offered by undertakings or solicited by competition authorities, remedies of data portability and data sharing may be used in such settings to structure the affected markets.[138] A link with the identified competition concerns is, however, necessary, so that the intervention remains purpose-specific.

II. Data Portability, Consumer Protection Law, and Beyond

After the adoption of the GDPR, a form of data portability has been put forward in the proposal for a Digital Content Directive,[139] published by the Commission in December 2015. This proposal would introduce a general-purpose tool, granting consumers some

[135] *See* Barbara Van der Auwermeulen, *How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations*, (2017) 33 COMPUTER L. & SECURITY REV. 57, 63 ("It cannot be excluded that article 102 of the TFEU may apply to some anti-competitive situations resulting from restrictions on data portability. Nevertheless, it appears to be challenging to apply European Competition Law to data portability.").

[136] *See* Inge Graef et al., *Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law*, INT'L DATA PRIVACY L. (forthcoming 2018).

[137] CJEU, European Comm'n v. Alrosa Co., Case C-441/07 P, ECLI:EU:C:2010:377, para. 48 (June 29, 2010).

[138] *See also* Costa-Cabral, *supra* note 130, at 511.

[139] *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*, COM (2015) 634 final (Dec. 9, 2015) [hereinafter *Proposal for a Digital Content Directive*].

degree of control over data in consumer protection law. Article 13(2)(c) of the proposal requires a supplier to provide a consumer who terminates a contract for the supply of digital content "with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent that data has been retained by the supplier." The provision goes on to state that the consumer is "entitled to retrieve the content free of charge, without significant inconvenience, in reasonable time and in a commonly used data format."[140] Interestingly, the proposal postulates an obligation of the supplier to refrain from the use of data retrieved by the consumer after contract termination.[141] This creates stronger property-like control over ported data than Article 20 of the GDPR, as the data must be removed from the service altogether.

As such, the proposal for a Digital Content Directive does not entitle consumers to have their digital content directly transmitted to a new provider. This difference from the RtDP under the GDPR can be explained by the distinct underlying objective of the Digital Content Directive. While the RtDP aims to give data subjects more control over their personal data generally, the relevant provisions in the proposal for a Digital Content Directive have the more specific objective to ensure that consumers benefit from effective protection in relation to the right to terminate the contract.[142] The extent of control granted to consumers under the data retrieval obligations of the Digital Content Directive is thus limited to cases of contract termination, but seems stronger in the level of control it confers. Nevertheless, as the proposal for a Digital Content Directive does not specify that data should be retrieved for a particular purpose for the data retrieval obligations to apply, it can be regarded as a general-purpose regime just like Article 20 of the GDPR.

When making a further comparison, it becomes clear that the scope of data covered under the data retrieval obligations of the proposal for a Digital Content Directive is broader than the type of data to which the RtDP of the GDPR applies. Unlike the latter—which covers

---

[140] *See id.* at art. 16(4)(b) (providing for a similar obligation for suppliers with regard to long term contracts for the supply of digital content). Interestingly, art. 16(4)(b) does not state that consumers are entitled to receive the content free of charge and thus seems to allow suppliers to ask for a fee.

[141] *See id.* at art. 13(2)(b)

> ([T]he supplier shall take all measures which could be expected in order to refrain from the use of the counter-performance other than money which the consumer has provided in exchange for the digital content and any other data collected by the supplier in relation to the supply of the digital content including any content provided by the consumer with the exception of the content which has been generated jointly by the consumer and others who continue to make use of the content.).

[142] *See id.* at recital 39 of the preamble.

only personal data provided by the data subject—the proposal for a Digital Content Directive also enables a consumer to retrieve any other data—to the extent that it has been retained by the supplier—generated by using the digital content which is not as such provided by the consumer. While the exact scope of data covered under the RtDP is still subject to debate, WP29 has made explicit in its guidelines on data portability that inferred data and derived data created by the data controller on the basis of data provided by the data subject falls outside the reach of the new right.[143] As examples of such excluded data, WP29 refers to data generated by a personalization or recommendation process and by user categorization or profiling.[144]

Judging from the phrasing of the relevant provisions in the Commission proposal for a Digital Content Directive, the data retrieval obligations might instead also apply to this kind of derived or inferred data, at least to the extent that this data has been retained by the supplier. In the General Approach adopted by the Council in June 2017, however, the scope of the data to which the retrieval obligations would apply is limited to "any digital content . . . to the extent that it does not constitute personal data, which was *uploaded or created by the consumer* when using the digital content or digital service supplied by the supplier."[145] This new formulation put forward by the Council seems to imply that derived or inferred data would not be included. It therefore remains to be seen how the legislative discussions evolve and what the final scope of the data retrieval obligations will be.[146] Their scope will determine the extent of protection for users but also the extent of the compliance burden for companies as well as the competitive impact of the Digital Content Directive on the market.

In this regard, one may wonder whether a consumer has an interest in receiving data that is further processed after it has been provided by the consumer or generated through a consumer's use of the digital content. In some cases, such a data retrieval obligation would be problematic in terms of its feasibility. Would suppliers, for instance, also be obliged to provide consumers with data that is further processed in an anonymized way, where re-identification of the consumer places a heavy burden on market players? This could also create tensions with the data protection regime, which instead encourages anonymization in order to further the fundamental right to data protection.[147] Reference can be made

[143] *See* discussion *supra* Section C.II.

[144] WP29, *supra* note 16, at 10–11.

[145] General Approach of the Council (June 8, 2017), art. 13a(3), http://data.consilium.europa.eu/doc/document/ST-9901-2017-INIT/en/pdf (emphasis added).

[146] *See also* Axel Metzger et al., *Data-Related Aspects of the Digital Content Directive*, 9 JIPITECH 90, 102–04 (2018) (comparing the RtDP in the GDPR and the data retrieval obligations in the Digital Content Directive).

[147] See *Opinion of the European Data Protection Supervisor 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content* 8–9, 18–20, (Mar. 14, 2017), https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (making

here to Article 11(1) of the GDPR, as already discussed above, which stipulates that data controllers are not required to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR, including the RtDP. The Council tried to solve these issues in its June 2017 General Approach in two ways. First, the Council excluded personal data from the scope of the data retrieval obligations. Second, the Council stipulated that a supplier is not required to make digital content available "to the extent that such digital content created by the consumer only has utility within the context of using the digital content or digital service supplied by the supplier, or which relates only to the consumer's activity when using the digital content or digital service supplied by the supplier or which has been aggregated with other data by the supplier and cannot be disaggregated or only with disproportionate efforts."[148]

Apart from its consistency with the GDPR, there is a need to weigh the interests of consumers and market players against each other. This is not to say that additional portability instruments should not be considered at all. Rather, this is a call for a clear goal-oriented approach in developing future regulation to prevent the adoption of new legislative or non-legislative measures without adequately examining the potential long-term effects on the market. With respect to the relationship between different portability instruments, several fields of EU law—such as data protection, competition, and consumer law—may certainly be applied together and complement each other in enforcing data portability. Nevertheless, one should prevent the situation where a wealth of different but related portability duties are imposed on market players who may struggle to understand what is exactly required under each area of law. There should be consistency between different EU initiatives involving some form of data portability.[149]

This is currently even more important, considering that portability is also emerging in legislative proposals targeting portability of non-personal data in a business-to-business setting. Article 6(1) of the Regulation on the free flow of non-personal data in the European Union establishes the Commission's role as follows:

---

recommendations to ensure that the Digital Content Directive does not change the balance found by the GDPR under which the processing of personal data may take place in the digital market); *see also* Natali Helberger et al., *The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law*, 54 COMMON MKT. L. REV., 1427–66 (2017) (discussing the relationship between data and consumer protection law more generally).

[148] General Approach of the Council, *supra* note 145, art. 13a(3).

[149] *See* ETNO Memo, *supra* note 112, at 9 (explaining—within the context of the GDPR and the EU electronic communications framework—that, "[w]hile the data protection oriented data portability right of the GDPR has a different scoping and orientation, one should be careful not to impose cumulative, redundant and potentially contradictory portability obligations on the telecoms industry.").

[To] encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, covering inter alia the following aspects: (a) best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data.[150]

As such, the applicability of the RtDP under data protection law—and the interpretation of its scope in line with its competitive impact—could be a blueprint for the development of future general-purpose portability tools under other regimes, including the Digital Content Directive and the Regulation on the free flow of non-personal data.

Naturally, there is also a need to align upcoming national implementations of EU legislation with new initiatives at the member state level. In this regard, it is worth referring to the French *Loi pour une République Numérique*—adopted on October 7, 2016—which introduces a data retrieval obligation for providers of online public communications services in French consumer protection law.[151] Such disparities—whereby one Member State imposes more far-reaching obligations on market players than others—should be avoided to prevent 28 different legal regimes concerning data portability from evolving in the EU. This will not only increase compliance costs for companies involved in cross-border activities but may also distort competition and put the achievement of the EU internal market at danger.

---

[150] *See Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union,* art. 6(1) (Nov. 9, 2018)*, http://data.consilium.europa.eu/doc/document/PE-53-2018-INIT/en/pdf*.

[151] *See* Art. L. 224-42-1 - L. 224-42-4 of Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Law 2018-132 of October 7, 2016 for a Digital Republic] JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [Official Gazette of France], Oct. 7, 2016, pp. 14–15 (stating that providers of online public communications service have to enable a consumer to recover free of charge all data that he or she has stored online—as well as all data resulting from the use of his or her user account that can be consulted online—with the exception of the data which has been significantly enhanced by the provider concerned). This provision resembles the data retrieval obligation that has been included in the proposal for a Digital Content Directive. The difference is that the latter is still under consideration in the EU legislative process while the former has already been adopted in its final form. As a result, regardless of what will happen to the relevant provisions in the proposal for a Digital Content Directive, providers of online public communications services in France have already had to comply with the data retrieval obligation set out in French consumer law as of the entry into force of the new duty enters in May 2018 (simultaneously with the start of the applicability of the GDPR).

Overview Of The Horizontal, Non-Sector-Specific Instruments Currently In Place Or In Development Enabling Some Form Of Data Portability*

Data type / Entitlement	Business-to-consumer (B2C)		Business-to-business (B2B)	
Personal data	**General purpose:** (1) GDPR: RtDP *(only covers personal data provided by the data subject)* (2) Proposal for a Digital Content Directive *(data retrieval obligations)***	**Specific purpose:** Competition law *(exploitation of consumers)*	**General purpose:** GDPR: RtDP *(only covers personal data provided by the data subject – applicable in a B2B setting as well when a business user acts as a natural person)*	**Specific purpose:** Competition law *(exclusion of competitors)*
Non-personal data	**General purpose:** Proposal for a Digital Content Directive *(data retrieval obligations)*	**Specific purpose:** Competition law *(exploitation of consumers)*	**General purpose:** Regulation on the free flow of non-personal data *(self-regulatory codes of conduct for facilitating the switching of providers)*	**Specific purpose:** Competition law *(exclusion of competitors)*

*Please note that the categorization in B2C and B2B in the table only considers the official scope of application of the different instruments. It is important to note, however, that the impact of an instrument targeted at enabling data portability in a B2C setting may also affect B2B relationships, and the other way around.

**While the data retrieval obligations in the Commission proposal for a Digital Content Directive apply to personal data, the General Approach of the Council excludes personal data from their scope.

F. Conclusions

This article set out to examine a horizontal, general-purpose regime for data portability as a new type of regulatory innovation from the perspective of the control that it confers.

We found that individuals get limited control over their personal data by invoking the RtDP under the GDPR. The right will mainly facilitate secondary data reuse among data controllers rather than individual data ownership. We contrasted this with upcoming data retrieval obligations in the proposal for a Digital Content Directive and the facilitation of data portability under competition law. The former is also designed as a general-purpose regime. It applies only upon termination of the contract but imposes more property-like control. The latter, which is the only one that pre-dates Article 20 of the GDPR, is strictly narrower, purpose-specific, offered on case-by-case basis, and does not offer RtDP-alike control over data. More conceptually, doubts also remain whether the RtDP fits the fundamental right to data protection or represents only a data-related form of regulation that aims to stimulate competition and innovation. The question is what the consequences of this will be for the implementation of the RtDP in practice. Data protection authorities may not feel comfortable with enforcing a right that is not of a traditional data protection nature. When asked, the Court of Justice, however, may decide to promote data portability as a new concept considering its expansive approach towards data protection in recent judgments.

An expansive interpretation of the RtDP will complicate its interface with IP law. There are a number of open questions regarding the extent to which companies will be able to invoke their IP rights on datasets to preclude data subjects from moving their personal data to another provider. As a result, the extent of control the RtDP will bring depends on how its balancing with IP law is conducted in practice. While the GDPR is designed as a general-purpose control mechanism that applies irrespective of the type of reuse of data, the reconciliation of the GDPR with IP rights might again limit the follow-on use of ported data by purpose-specific considerations.

The discussion also shows that there is a risk that data portability regimes emerge with only loosely defined justifications and thus easily become a goal in and of themselves. Moreover, with a growing number of policy interventions, there is a strong need to consider the consistency of legal instruments internally and with each other.